Externalizing Europe: the global effects of European data protection

Bendiek, Annegret; Römer, Magnus

Postprint / Postprint
Zeitschriftenartikel / journal article

Bendiek, Annegret; Römer, Magnus

Article — Accepted Manuscript (Postprint)

Externalizing Europe: the global effects of European data protection

Digital Policy, Regulation and Governance

Provided in Cooperation with:
WZB Berlin Social Science Center

Suggested Citation: Bendiek, Annegret; Römer, Magnus (2019) : Externalizing Europe: the global effects of European data protection, Digital Policy, Regulation and Governance, ISSN 2398-5046, Emerald, Bingley, Vol. 21, Iss. 1, pp. 32-43, http://dx.doi.org/10.1108/DPRG-07-2018-0038

This Version is available at:
http://hdl.handle.net/10419/210482

Externalizing Europe: the global effects of European data protection

Annegret Bendiek and Magnus Römer

Abstract

Purpose – This paper aims to explain how the EU projects its own data protection regime to third states and the US in particular. Digital services have become a central element in the transatlantic economy. A substantial part of that trade is associated with the transfer of data, most of it personal, requiring many of the new products and services emerging to adhere to data protection standards. Yet different conceptions of data protection exist across the Atlantic, with the EU putting a particular focus on protecting the fundamental right to privacy.

Design/methodology/approach – Using the distinction between positive and negative forms of market integration as a starting point (Scharpf, 1997), this paper examines the question of how the EU is projecting its own data protection regime to third states. The so-called California effect (Vogel, 1997) and the utilization of trade agreements in the EU's foreign policy and external relations are well researched. With decreasing effectiveness and limited territorial reach of its enlargement policy, the EU found trade agreements to be particularly effective to set standards on a global level (Lavenex and Schimmelfennig, 2009). The existence of the single market makes the Union not only an important locus of regulation but also a strong economic actor with the global ambition of digital assertiveness. In the past, establishing standards for the EU's vast consumer market has proven effective in compelling non-European market participants to join.

Findings – As the globe's largest consumer market, Europe aims to project its own data protection laws through the market place principle (lex loci solutionis), requiring any data processor to follow its laws whenever European customers' data are processed. This paper argues that European data protection law creates a ''California Effect'', whereby the EU exerts pressure on extra-territorial markets by unilateral standard setting.

Originality/value – With its GDPR, the EU may have defused the problem of European citizens' data being stored and evaluated according to the US law. However, it has also set a precedent of extra- territorial applicability of its legislation – despite having previously criticized the USA for such practices. By now, international companies increasingly store data of European customers in Europe to prevent conflicts with EU law. With this decision, the EU will apply its own law on others' sovereign territory. Conflicts created through the extra-territorial effects of national law may contradict the principle of due diligence obligations but are nevertheless not illegitimate. They may, however, have further

unintended effects: Other major economies are likely to be less reluctant in the future about passing legal provisions with extra-territorial effect.

1. Introduction

The trade in digital technology and services has become a central element of international economic relations[1]. Since 2014, more than half of services traded between the EU and US are digital (Meltzer, 2014). A substantial part of this trade is associated with the transfer of data, some of it personal, some of it machine generated. Emerging technologies such as 5G and the "Internet of Things", as well as growing middle classes worldwide are set to further increase digital trade. Despite this, conflicts have arisen over how to use those growing amounts of data, giving way to conflicting regulatory approaches. Calls for "data sovereignty", i.e. enhanced control of data controllers over data have increased (Otto et al., 2016; Cory, 2017). Competition law is increasingly applied to tackle growing data-monopolies. In addition, data protection law has become the primary mode of regulation to those segments of traded data, which can be related to individuals. To ensure that individuals remain protected in an international data economy, EU legislators have created two safeguards: The lex loci solutionis ("Law of the place where relevant performance occurs") requires any data processor to follow the EU's General Data Protection Regulation (GDPR) whenever European customers' data are processed. To give additional protection to data which are transferred abroad, GDPR principles have become enshrined into international trade agreements. Preeminent examples of the latter are the EU-US Privacy Shield, or relevant parts of the recently signed EU-Japan Economic Partnership Agreement ("Jefta," for Japanese-European Free Trade Agreement). All of those agreements are subjected to the GDPR. In spite of this, both mechanisms are devised to protect European customers. Nevertheless, most globally operating digital service providers claim that they will adhere to GDPR standards globally, granting all their customers the same level of data protection. The GDPR's reach therefore seems to extend beyond the European market and its customers. By setting the standards for the largest consumer market worldwide, it pressures globally operating firms to adopt its principles for all their customers. This paper aims to explain this process, thereby also outlining potential conflicts arising from such modes of global rule making.

To date, much of the conflicts on international data protection occur across the Atlantic, between the two biggest economies and trading partners of the world. Often, those conflicts are articulated in judicial decisions, restricting the options for legislators. The EU's binding Charter of Fundamental Rights predetermines a solid frame for policy-making, with the European Court of Justice not hesitating to remind European Commission, Council and Parliament of safeguarding citizens' basic rights. The first conflicts over

data protection led to trade negotiations in the 1990s, which were only seemingly resolved by the Safe-Harbour Agreement in 2000 (Whitman, 2004). The issue reemerged in the wake of the NSA revelations by Edward Snowden (Bendiek, 2014). In October 2015, the European Court of Justice (ECJ) overturned the Commission's Safe-Harbour Agreement not adequately protecting EU citizens' right to privacy. In early February 2016, the European Union and the USA agreed to replace Safe Harbour with the EU-US Privacy Shield. Yet conflicting conceptions of privacy and data protection are not exclusive to transatlantic trade. With digital business growing globally, newer markets inevitably enter trade relations with the EU. Conflicts over data transfers with India, the Mercosur and the European neighborhood are on the horizon (European Commission, 2017).

Using the distinction between positive and negative forms of market integration as a starting point (Scharpf, 1997), this paper examines the question of how the EU is projecting its own data protection regime to third states. The so-called California effect (Vogel, 1997), as well as the utilization of trade agreements in the EU's foreign policy and external relations, are well researched. With decreasing effectiveness and limited territorial reach of its enlargement policy, the EU found trade agreements to be particularly effective to set standards on a global level (Lavenex and Schimmelfennig, 2009). The existence of the single market makes the Union not only an important locus of regulation but also a strong economic actor with the global ambition of digital assertiveness. In the past, establishing standards for the EU's vast consumer market has proven effective in compelling non-European market participants to join.

In chapter two, after outlining the significance of international data transfers and trade for the global economy, the article proceeds by briefly describing its theoretical approach in chapter three. In chapter four, the European conception of data protection and privacy will be presented, with a particular focus on recent judicial decisions and legislative reform. Chapter five will exemplify possible conflicts arising from national or regional laws being applied to global markets by example of the GDPR and the CLOUD Act. Chapter four will summarize the findings and point out future challenges for international data transfers.

2. The growth in digital services trade

The growth of the internet has enormously expanded the importance of data transfer and the trade in services involving data protection. Today, data are transferred as a side effect of the use of digital services, for example data transfer involved in using digital insurance services. Moreover, data are not only utilized by multinationals managing decentralized production in global value chains, but are the very essence of online platforms offering

services in communication, product development and, crucially, targeted advertisement (Christl, 2017; Bennett, 2012)[2].

Part of this transferred data encompass machine data, i.e. data produced by jet engines, lifts or cars, whose export thus implies data transactions in the service sector, for example, as the basis for repair and maintenance work. The rules applied to such data will shape the provision of this kind of after-sales services: retaining it will enable an exporter to conduct maintenance work as a service export. Using and analyzing the data generated and exchanged by digitally networked products, such as fridges and thermostats, on the "Internet of Things" requires free international exchange. Yet the term "machine data" often conceals persisting personalization: although generated by machines, such data still reveal information about the individual user. Additionally, it is problematic to assume that consumers truly approve the use and processing of such a plethora of personal data only because they use the products gathering such data. In reality, consumers often lack the skills required to understand privacy mechanisms. Their interest in using the services on offer outweighs their knowledge about data protection (Hofmann and Bergemann, 2017).

In view of the rapidly growing role of IT goods and services, the USA possesses a strong interest in free international exchange of data, but so do important parts of the European economy. Digital services such as e-consulting are becoming increasingly important. They already represent more than 50 per cent of transatlantic service exports (USA 72 per cent, European Union 63 per cent) and they supply important production inputs for export goods (Meltzer, 2014). Significant sectors of industry are interested in exporting these products, as well as improving their access to imports that help them to lower their costs and improve their competitiveness. Transatlantic relations in connection with "computer services" touch on practically all commercially used personal data. According to the USA International Trade Commission (USITC), the internet reduces average trading costs by 26 per cent. Especially in developing countries, the market for digital services is set to grow considerably. Large parts of the world will join the internet using mobile devices, 54 per cent of which will be "smart" by 2018 (up from 21 per cent in 2013).

3. Trading up of data protection law

In European data protection law, it is the EU which has become the champion of consumers, supporting their rights even if that means confronting the big tech companies of the Silicon Valley. Already in the negotiation processes for the first common rules on data protection, which culminated in the Data Protection Directive in 1995, consumer rights were emphasized. While common rules should ease transnational data flows, they should also strengthen the individual fundamental right to privacy both vis-a`-vis the state and

private actors (Gonza´lez Fuster, 2014). As a result, European Data Protection Law exemplifies both positive and negative forms of integration (Scharpf, 2002). It is negative, or market making, by homogenizing the patchwork regulations which had limited intra-European data transfers prior to common legislation. It is positive, or market shaping, by granting rights to data subjects and creating obligations for data processors.

The EU enshrined both privacy and data protection in its Charter of Fundamental Rights, in Art. 7 and Art. 8, respectively. Its General Data Protection Regulation (GDPR) gives robust individual rights to the so-called data subject. EU data protection legislation hence introduced additional rules for market actors, aiming to empower consumers vis-a`-vis producers (as well as citizens vis-a`-vis the state) and weaker market participants across jurisdictions (Börzel et al., 2003). The effects of these European regulations on the US market are stunning to many observers. "Ironically, many Americans are going to find themselves protected from a foreign law", said Rohit Chopra, the Democratic commissioner at the Federal Trade Commission (FTA) (Romm et al., 2018). The EU has emerged as the most powerful regulator of Silicon Valley, "stepping in where Washington has failed or simply has been unwilling – to limit some of the United States' most lucrative and politically influential companies" (ibid.).

3.1 Explaining trading up

How could this happen? How to understand that the politically divided EU exerts such a strong influence on the largest digital economy of the world which hosts the most sophisticated producers of high-end technology? An important explanation for this process has been forwarded by David Vogel (1997). In "Trading Up", Vogel aimed to show the beneficial effects of free trade on consumer protection, arguing that free trade will often lead to stronger and more consumer-friendly regulations. He based his claim on three arguments. First, stiffer regulations may strengthen the competitive advantage of firms, thus providing strong incentives to implement them even if they produce additional costs. Second, large import markets can set product standards unilaterally and compel outsiders to meet them if they are to benefit from exports. Finally, to the extent that markets are governed by parties that are sensitive to consumer concerns, their governments often have negotiated international agreements that foster their implementation.

Especially the two latter arguments, relating to the power of markets and the importance of international agreements, are insightful for understanding the effects of European data protection law on the US market. Following Vogel, we can observe the working of a so-called California effect. The term refers originally to the introduction of new regulations in California in the 1980s, proscribing rigid and environmentally friendly standards for car emissions. In order not to lose the (huge) Californian market, American car manufacturers

were confronted with the options of either accepting the additional production costs of two different standards (one for California and one for the rest of the world) or to universalize the more rigid standards. The outcome is well known. It took the car manufacturers of the USA, and a little later of the rest of the world, little time to understand that implementing one standard, and serving one market, is cheaper than two, even if that implies adhering to higher standards overall.

The same exists today with regard to the comparatively rigid European data protection law. For global companies like Google, Facebook or Amazon, it is not an option to leave the European market. At the same time, it is an extraordinary burden to organize their business along two different sets of legal regulations. The inherent mobility of data necessitates de facto transnational regulation. For now, it is far more efficient to implement the rigid European regulations on a global scale, instead of trying to align digital markets with national borders.[3] As a result, the large providers of digital services claim to offer to the American consumer the same level of protection as they do for Europeans customers. The outcome is straight forward: although legally only aiming to safeguard EU customers who rely on foreign based services, the EU de facto extends the territorial reach of its data protection law, forcing foreign market participants to obey EU law irrespective of whether they serve EU, US or any other customers.

Yet from the EU's perspective, this indirect effect of European law on extraterritorial markets is not sufficient. Acknowledging the mobility of data and the importance of US digital service providers, the EU is additionally negotiating international agreements to ensure that EU customers' data is also protected when processed abroad, outside of its own jurisdiction. While not forcing third states to adopt EU legislation, adequacy agreements nevertheless aim to ensure that the third state's level of data protection is adequate, i.e. grants similar rights as EU law does.

3.2 Justifying external effects

This approach is not without criticism. Scholars have repeatedly warned of a regulative fragmentation, in which conflicting national legislation on the transnational policy field of internet governance may limit the internet's openness (Mueller, 2017; Reinsch, 2018). For overcoming friction in transatlantic market making, the strict application of the principle of due diligence might bridge the gap in the transatlantic digital economy. Due diligence derives its particular normative force from the idea that states are not only responsible for keeping law and order on their own territories, but also bear responsibility for the external consequences of internal regulations (Bendiek, 2014). As we have seen, decisions taken by individual states increasingly have an impact beyond their national territory. That is why the principle claims that states must exercise care with such decisions and be

accountable to one another for them. As far as the internet is concerned, states in cooperation with other states are obliged to do everything that may be reasonably expected of them to help deliver an "open, free and secure Internet".

Due diligence is an important principle in all matters relating to international relations. It safeguards that states do not violate their mutual interests but treat each other respectfully. It is doubtful, however, whether the principle pays sufficient attention to the asymmetrical character of global market making and its direct effect on individual citizens. The global polity has a striking imbalance between well-organized capital interests, on the one hand, and diffuse consumer interests on the other (Olson, 2003). Market-making follows the path of negative integration (Scharpf, 2002) and has become largely disembodied from political control and ambitious social standards (Ruggie, 1982). The interests of consumers are therefore easily neglected and, in the absence of unilateral state interventions, more often than not subject to a regulatory race to the bottom (Delaware-effects). The alternative to EU external effects is thus not democracy or any other form of good governance but the dominance of market processes and disrespect for consumer concerns. Justifying the EU's external effects is thus coterminous with defending the right of global consumers to digital services that live up to the best standards of privacy and protection. This paper describes the process of externalizing EU governance by showing why and how the EU disseminates its data protection principles in the global digital economy. To this end, official trade agreements, key legislative acts and judicial decisions tackling the issues of data sovereignty, data protection and data transfers will be analyzed.

4. The European conception of data protection

After the OECD issued its non-binding Privacy Guidelines in 1980, the Council of Europe adopted the first legally binding Convention on Data Protection in 1981. In the following years, datafication increased, and European policy makers acknowledged the needs for regulating data protection at EU level. By the early 1990s, Parliament and Commission began to negotiate the Data Protection Directive. While Parliament stressed the fundamental rights dimension of data protection, the Commission focused on the market making function, which common data laws would have (González Fuster, 2014). The Directive was adopted in 1995, displaying both the positive and negative dimensions of data protection, aiming "to protect the fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of personal data" as well as to ensure the "free flow of personal data between Member States". A Directive on privacy and electronic communications (ePrivacy Directive) followed in 2002, supplemented in 2009 with a cookie law to protect personal data generated in the form of cookies when using the internet.

Apart from legislation, privacy rights were further strengthened by the ECJ. Following Edward Snowden's revelations about the extent of NSA surveillance, the Facebook critic Maximilian Schrems took the Irish data protection authority to court in June 2013, challenging the authorities' claim that his data was sufficiently safeguarded by Facebook. In April 2014, the ECJ ruled general data retention unlawful, contradicting EU secondary legislation which had required all member states to pass data retention laws (C-203/15 and C-698/). In May 2014, the ECJ formulated the "right to be forgotten" in another judgement (C-131/12), stating that search engines must adhere to data protection law and cannot fall back on American law, even if the parent company is headquartered in the USA and its data are processed there. Following the decision, EU citizens now have the right to demand for the search engines to delete their personal information. The ECJ's Safe Harbour ruling (C-362/14) of October 2015 supported Schrem's view and demanded a reformation of the transatlantic data transfer agreement Safe Harbour, to ensure sufficient protection of EU customers' privacy as a fundamental right (Carrera and Guild, 2015). In mid-December 2015, three years after the Commission had published its initial draft law, the European Parliament, the Council of Ministers and the Commission passed the GDPR, in co-decision, leaving a two-year implementation phase before it entered into force in May 2018. The Regulation applies to all processors of personal data, both public and private. Yet there are exceptions: In certain particularly sensitive areas such as education or health, member states can draw data localization laws, in order to avoid sensitive data being transferred abroad. In addition, the police and judicial system is excluded, and is covered by its own new data protection directive, which was negotiated simultaneously. The GDPR was meant to be accompanied by the e-Privacy Regulation, which would offer the same safeguards to all forms of electronic communication. However, conflicts over how to regulate online tracking technologies have delayed the legislative process – by now it seems unlikely to pass Council and Parliament before the European Parliament's election in May 2019.

Both European legislative and judicial developments in recent years have hence strengthened an inherently positive and negative conception of data protection. Data transfers are seen as crucial to revive the slowing European economy. Moreover, the fundamental rights to privacy and data protection are increasingly understood as vital for liberty and democracy (Bennett, 2012). In liberal societies, the argument goes, the right to privacy is constitutive, for without privacy there can be no liberty. Although in the US privacy and civil liberties are closely related too, USA data protection and privacy laws have a different focus. In the USA, the focus is not on the protection of human dignity, but on freedom in the sense of liberty as a civil right of the individual, who wishes to be "free of legal regulations" (Bendiek et al., 2015).

4.1 The general data protection regulation

The GDPR brings for the first time harmonized, directly binding data protection law throughout the European Union and is intended to avoid member states competing to offer the weakest protections. “European law on European soil” is the Commission’s motto. The GDPR keeps many of the cornerstones in European data protection law, including the requirement to obtain users’ explicit consent if personal data is collected, the limitation to use the data only for predetermined purposes and the principle to collect as little data as possible. Users’ rights to have stored information deleted (the right to be forgotten) and to take their data from one provider to the next (portability) are also enshrined in the GDPR. Data subjects will further gain the right to object to automated decision making. Companies will have to supply products with data-protection-friendly default settings (privacy by design and by default). New data protection and security requirements will promote IT products whose technological configuration facilitates the protection of private data. Additionally, data controllers will have to prove that they undertake appropriate safeguards by conducting data protection impact assessments (DPIA) and recording their use of personal data. Many of those principles have not yet been put into practice and are heavily contested. Their ultimate implementation will be a result of negotiations between supervisory authorities, legal scholars and data processors, many of which will ultimately be decided in court.

Certain aspects of the GDPR have attracted criticism. In the European Union, data processing is tied to a defined purpose that limits its application, a principle unknown in the USA. The proposed limitations fundamentally contradict the business logic of online platforms like Facebook and Amazon, since big data applications systematically subvert the concept. Big data’s basic logic is to gather and analyze enormous quantities of data and then to use it for many different purposes, rather than repeatedly for the same purpose. In fact, it is frequently statistical analysis of big data that generates new possibilities for using personal data in the first place. Big data technologies further endanger pseudonymization and anonymization processes, since individuals can often be re- identified by analyzing and triangulating enough data (Mayer-Schönberger and Cukier, 2013). Also the GDPR’s segments on automated decision making, often discussed as “algorithmic” or “robotic” decision making received heated debate, with critics both arguing it would stifle innovation or curb individual freedoms. Many still put hope into DPIAs as a process oriented solution, which could provide enough flexibility to reconcile rapid technological change with static regulatory principles.

Independent national data protection authorities will be crucial for the successful implementation of the GDPR. They are fulfilling an increasingly important regulatory and complaint-handling role, monitoring how personal data is used in the information society

and imposing sanctions as necessary. Firms from third states which operate within the EU's market will also have to obey the new European rules, with violations subject to fines of up to 4 per cent of annual turnover or 20 million euro – whichever is higher. The ECJ has emphasized the need for "complete independence" of data protection authorities in order to ensure effective protection of the data subject's rights (518/07). Through consistency and cooperation mechanisms, companies will be addressed by a single lead authority and consumers wishing to lodge complaints against providers in other EU member-states will be able to do so in their own language through the relevant agency in their own country. Through their European forum, the European Data Protection Board, which gathers authorities' representatives from all 28 member states, data protection authorities will gain considerable powers. Acting with a simple majority, the EDPB can issue decisions on landmark cases and settle conflicts on data protection principles.

For international data transfers, two elements of the GDPR are especially important: its territorial scope and its requirements for adequacy clauses. Regarding the GDPR's territorial scope, the legislators aimed to account for the international character of many digital services. To ensure that European customers would also be protected when using services from companies abroad, the GDPR covers all processing of personal data within EU borders, as well as all processing of EU customers' data abroad, if the company directly targeted or advertised to customers residing in the EU. This extended territorial scope has attracted criticism, especially for the enforcement problems it creates (Kuner, 2015).

The GDPR additionally re-orders the mechanism for international data transfers. Carrying the exclusive competence for external trade, also under the GDPR, the Commission is responsible to negotiate adequacy agreements. Apart of binding corporate rules, adequacy agreements are the EU's principal way to formulate rules on international data flows. Adequacy agreements allow transfers of personal data to third countries, if the country's level of data protection is equivalent to the EU's. Already under the Data Protection Directive from 1995, adequacy agreements existed, albeit mostly focusing on the adequacy of the third state's legal provisions (Bennett, 2012). Under the GDPR, and as a consequence of the ECJ's "Schrems" decision, adequacy agreements include both the de jure as well as de facto dimensions, meaning that also the regulatory oversight over the third state's data protection and privacy laws must be taken into account. Under the GDPR, the Commission must consult the European Data Protection Board when concluding an adequacy agreement, opening the EDPB a chance to demand the creation of similar oversight structures as they exist in the EU. Every four years, the Commission must reevaluate the agreements, ensuring that protection levels have remained adequate. An adequacy finding also serves as the basis for transatlantic arrangements such as the EU–USA Privacy Shield.

4.2 Trade agreements and data protection

International agreements on data trade are not exclusively covered by EU initiatives. Trade in services is regulated by the WTO's General Agreement on Trade in Services (GATS) of 1995, while a separate Information Technology Agreement abolishes tariffs on listed IT products (Schmieg and Bendiek, 2016). GATS involves general duties: All trading partners must be treated equally, transparency standards must be implemented and service providers must be granted the same treatment as their domestic counterparts. The liberalization duties of individual WTO members are listed in so-called schedules (Schmieg and Bendiek, 2016). GATS distinguishes four modes of supply of trade in services. Although numerous electronic services did not yet exist when GATS came into force, many are nonetheless covered by the GATS classification. Certain services can be provided both digitally and by other methods.

Many aspects of trade in digital services touch on questions of data protection in dimensions that were inconceivable when the GATS was drawn up in 1995. Today, the coordination of the various national data storage regimes is rudimentary or non-existent, and their relationship to international trade law is unclarified. The exceptions laid out in GATS form the legal basis for data protection rules. GATS Article III permits parties to keep information confidential in specific circumstances such as public interest, while GATS Article XIV (General Exceptions) underlines the right of parties to adopt and enforce laws and regulations. This also applies to the protection of privacy in relation to the processing and dissemination of personal data. The GATS Annex on Financial Services, section 2 (Domestic Regulation) specifies that parties are under no obligation to reveal information relating to individuals' business bank and accounts, or to confidential and other information in the possession of public entities. GATS created the basis for a further liberalization of trade in services, which was originally to take place at the multilateral level. However, not all the parties were interested in further opening their service sectors. Currently, as a result, only plurilateral talks on a Trade in Services Agreement (TiSA) are being conducted under the auspices of the WTO. The European Union is negotiating on new principles for domestic regulation of ICT services (including cross-border data transfers), electronic commerce and computer-related services.

In relation to data protection, the European Commission emphasizes that TiSA will contain the same safeguards as GATS. At the same time, it argues that the data transfer rules discussed for TiSA are inspired by similar provisions in existing free trade agreements, for example with South Korea. Article 7.43 of the latter agreement explicitly states that both parties should develop appropriate privacy protection rules, especially in relation to the transfer of personal data. As such, the South Korea FTA goes further than previous exceptions, regarding the proposed rules not as possible exemptions from free trade, but

stressing the need to develop adequate safeguards in the first place. However, critics fear that the USA has already asserted its own diverging interests in the TiSA talks, and that TiSA will provide for free data transfer between its signatories.

4.3 Safe harbour, privacy shield and other "adequacy agreements"

The Safe-Harbour Agreement was adopted in 2000. It was designed to ensure that US companies give adequate protection to European users' privacy when they process their data stateside (Monteleone, and Puccio, 2017). De facto, although not de jure, this was a decision by the Commission, in which it classified companies that agreed to observe particular data protection standards and submit to controls by the US Federal Trade Commission (FTC) as safe harbors. The former FTC Commissioner Julie Brill pointed out that in the fifteen years of its existence just four reports of violations had been received from European data protection authorities, while altogether 4,400 US companies had registered on the basis of the agreement. During the same period, she said, the FTC had investigated numerous violations and initiated legal action in 39 cases, including against Facebook. However, critics point out that the small number of legally relevant cases could also imply Safe Harbour's weak effectiveness because it complicates complaints for affected individuals.

In October 2015, the ECJ ruled Safe Harbor invalid. The Court based its verdict on the Treaty of Lisbon and the EU's Charter of Fundamental Rights. Data protection, the verdict read, was a fundamental right enabling the superior right of privacy. Consequently, the verdict underlined the crucial role of national data protection authorities, their independence, and their right to assess and intervene in international data transfers (Carrera and Guild, 2015). The Court singled out US government access to European users' data for particular criticism.

Following the decision and under pressure of the European forum of national data protection authorities, the European Union and the USA agreed to a new arrangement for data exchange: the EU-US Privacy Shield. Under the agreement, the US Department of Commerce will monitor US companies processing data from Europe. In other words, the US side agreed to regulation conducted by its own authorities. The two partners will review the agreement's implementation annually. Anyone who believes their data privacy rights have been violated on account of US national security interests will be able to turn to an ombudsman operating independently of the US security agencies. In case of conflict, there will be a free mediation process. Such relatively complicated and ineffective enforcement and oversight will produce legal insecurity in the medium term.

In addition to the EU–US privacy shield, the EU has adequacy agreements with Andorra, Argentina, Canada (restricted to commercial organizations), the Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay. Within the negotiations over JEFTA, also Japan will soon be included in this list, with South Korea being the most likely follow up (European Commission, 2018c, 2018b). Current negotiations over a free trade agreement with Indonesia have further shown that the Commission will ultimately put data protection above the free flow of data, arguing that as a fundamental right, it is "not negotiable" (European Commission, 2018a).

5. Conclusions

Data protection is today one of the most important policy fields for states to reassure their sovereignty online. The EU has become a major player in this area. It has one of the biggest consumer markets worldwide and is self-confidently using its policy-leverage for promoting its citizens' and consumers' desire for privacy and data protection, even if that conflicts with the interests of its trading partners. The conflict between Europe and the US on this issue is symptomatic, in that it merged questions of trade, regulatory oversight and fundamental rights. Different conceptions of privacy and conflicting interests in trade and regulatory affairs will persist, not only across the Atlantic, but in all international digital trade relations.

Most of the current debate takes place on the transatlantic level. Yet, frictions over the matter of international data transfers are likely to increase globally. Once more, businesses from emerging economies aim to serve European customers. To date, most transnational digital business activities take place between established democracies. Although differences in the conceptions of data protection and privacy exist, those states understand the importance of both in principle – and have developed certain safeguards for data subjects. To acknowledge privacy rights of data subjects will remain a fundamental precondition for anyone operating in the European market, as will appropriate oversight bodies. Either way, with digital markets expanding in territorial scope, international norms of data protection will have to be developed. The existing patchwork of agreements does not answer the question of how to reconcile free data flows with the fundamental right to privacy exhaustively. However, it is opening the door for future legal integration.

The need for international agreements and oversight bodies to avoid regulatory fragmentation and to increase regulatory effectiveness will rise. With data protection becoming ever more relevant for all digital matters, it may learn a lesson from internet governance, become more transnational and include more stakeholders. The European system is well

equipped to become a role model in this regard, since data protection authorities already cooperate closely with companies in order to support an efficient implementation process.

With its General Data Protection Regulation, the EU may have defused the problem of European citizens' data being stored and evaluated according to US law. However, it has also set an influential precedent of extra-territorial applicability of its legislation – despite having previously criticized the US for such practices. By now, international companies increasingly store data of European customers in Europe to prevent conflicts with EU law. With this decision, the EU will apply its own law on others' sovereign territory. Conflicts created through the extra-territorial effects of national law may contradict the principle of due diligence obligations but are nevertheless not illegitimate. They may, however, have further unintended effects. Other major economies are likely to be less reluctant in the future about passing legal provisions with extra-territorial effect. This could result in a collision course for different national legal systems, which would encourage the fragmentation of the global economic space and the Internet. The Privacy Shield and the transatlantic agreement on data protection in criminal cases are therefore vital steps in the effort to stop this process.

Indeed, conflicts over data flows have also emerged in other policy areas: When in 2013 Microsoft denied the FBI access to communication data stored in Ireland, a year long legal battle followed, in which the US Software giant was caught between conflicting legislations, ultimately arguing that it saw no legal obligation to forward data stored on foreign soil to US services. The conflict was only settled in 2018, when the Clarifying Lawful Overseas Use of Data Act or CLOUD Act was pushed through Congress without a parliamentary hearing, giving US investigators worldwide access to servers owned by US companies. The CLOUD Act also expressly stipulates that the USA must enter into government agreements with foreign states that allow foreign investigative authorities access to data stored by US companies. In return, US investigators will also have access to data stored in the respective country. Yet by only allowing for bilateral agreements with national governments, the CLOUD Act circumvents the EU as a possible contracting party. The EU, as well as its member states however prefer to find an agreement between the EU and the US.

The CLOUD Act hence demonstrates similar complexities and possible conflicts surrounding unilateral legislation as the GDPR does. While both contain passages stipulating the creation of international agreements and contracts, they simultaneously aim for extraterritorial and even global reach. While their goals – privacy protection and effective law enforcement – are fully legitimate, they open the gate for future conflicts on the regulation of the digital economy. Legislators are well advised to pay more attention to the due-

diligence norm when unilaterally drafting rules for the digital economy. Due diligence stresses the cooperative, inclusive and transparent global character of good international governance, without concealing their domestic foundations. It should be considered to be the lowest common denominator in international relations and seems to be a suitable approach for transnational data flows.

Notes

1. Parts of this article are based on SWP comments, published as Bendiek, A. and Schmieg, E. (2016), European Union Data Protection and External Trade: Having the Best of Both Worlds?, Berlin. See: https://www.swp-berlin.org/en/publication/eu-data-protection-and-external-trade/
2. Focusing on data transfers in relation to international trade policy, this paper does not discuss data transfers between national authorities.
3. Whether this cost-benefit calculation will hold in the long term, largely depends on how strict the GDPR will be enforced within the EU. A strict enforcement could well alter the calculation, creating a de facto transatlantic division in consumer rights.

References

Bendiek, A. (2014), "Tests of partnership: transatlantic cooperation in cyber security, internet governance, and data protection", Transatlantic Academy Paper Series, 2013-2014 No. 1.

Bendiek, A., Berlich, C. and Metzger, T. (2015), The European Union's Digital Assertiveness, SWP Comments.

Bennett, C.J. (2012), "The Geo-Politics of personal data", available at: www.hir.harvard.edu/article/?a=3016

Börzel, T., Hofmann, T. and Sprungk, C. (2003), "Einhaltung von recht jenseits des nation-alstaats. Zur implementationslogik marktkorrigierender regelungen in der EU", Zeitschrift Für Internationale Beziehungen, Vol. 10 No. 2, pp. 247-286.

Carrera, S. and Guild, E. (2015), "The end of safe harbor: what future for EU-US data transfers?", Maastricht Journal of European and Comparative Law, Vol. 22 No. 5, pp. 651-655. Christl, W. (2017), Corporate Surveillance in Everyday Life, Vienna.

Cory, N. (2017), Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?,

European Commission (2017), "Communication from the European commission to the European parliament and the council. Exchanging and protecting personal data in a globalised world",

European Commission (2018a), "EU provisions on cross-border data flows and protection of personal data and privacy in the digital trade title of EU trade agreements", available at: www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=2ahUKEwj5t_z5tbrcAhVHLsAKHaOOBegQFjABegQIBBAC&url=http%3A%2F%2Ftrade.ec.europa.eu%2Fdoclib%2Fhtml%2F157129.htm&usg=AOvVaw2z_aEhpgfCS7mpdbg5Ukak

European Commission (2018b), The European Union and Japan Agreed to Create the World's Largest Area of Safe Data Flows, Tokyo.
European Commission (2018c), "Adequacy decisions", available at: www.ec.europa.eu/info/law/law-topic/ data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en
González Fuster, G. (2014), The Emergence of Personal Data Protection as a Fundamental Right of the EU, Law, Governance and Technology Series, Vol. 16, Springer International Publishing, Cham, s.l.
Hofmann, J. and Bergemann, B. (2017), "Die informierte einwilligung: ein datenschutz-phantom", 1 June, available at: www.netzpolitik.org/2017/die-informierte-einwilligung-ein-datenschutzphantom/
Kuner, C. (2015), "Extraterritoriality and regulation of international data transfers in EU data protection law", International Data Privacy Law, Vol. 5 No. 4, pp. 235-245.
Lavenex, S. and Schimmelfennig, F. (2009), "EU rules beyond EU borders: theorizing external governance in European politics", Journal of European Public Policy, Vol. 16 No. 6, pp. 791-812.
Mayer-Schönberger, V. and Cukier, K. (2013), Big Data: A Revolution That Will Transform How we Live, Work and Think, 1. publ, Murray, London.
Meltzer, J.P. (2014), "The importance of the internet and transatlantic data flows for US And EU trade and investment", Working Paper.
Monteleone, S. and Puccio, L. (2017), "From safe harbour to privacy shield: advances and shortcomings of the new EU-US data transfer rules", available at: www.europarl.europa.eu/RegData/etudes/IDAN/ 2017/595892/EPRS_IDA(2017)595892_EN.pdf
Mueller, M.L. (2017), Will the Internet Fragment?: Sovereignty, Globalization, and Cyber-space, Digital Futures Series, Polity, Cambridge, UK, Malden, MA.
Olson, M. (2003), The Logic of Collective Action: Public Goods and the Theory of Groups, Harvard Economic Studies, Vol. 124, Harvard Univ. Press, Cambridge, MA, p. 21.
Otto, B., Auer, S., Cirullies, J., Ju¨ rjens, J. and Menz, N. (2016), "Industrial data space: digital sovereignity over data", White Paper.
Reinsch, W.A. (2018), "A data localization free-for-All?", available at: www.csis.org/blogs/future-digital- trade-policy-and-role-us-and-uk/data-localization-free-all
Romm, T., Timberg, C. and Birnbaum, M. (2018), "New laws make Europe a regulator of U.S. privacy", The Washington Post, available at: www.viewer.factiva.com
Ruggie, J.G. (1982), "International regimes, transactions, and change: embedded liberalism in the postwar economic order", International Organization, Vol. 36 No. 2, pp. 379-415.
Scharpf, F.W. (1997), "Balancing positive and negative integration: the regulatory options for Europe", MPIfG Working Paper, No. 8.

Scharpf, F.W. (2002), Governing in Europe: Effective and Democratic?, 1. publ., repr, Oxford University Press, Oxford.
Schmieg, E. and Bendiek, A. (2016), European Union Data Protection and External Trade: Having the Best of Both Worlds?, Berlin.
Vogel, D. (1997), Trading up: Consumer and Environmental Regulation in a Global Economy, 2. printing, Harvard Univ. Press, Cambridge, MA.
Whitman, J.Q. (2004), "The two Western cultures of privacy: dignity versus liberty", Yale Law Journal, Vol. 113 No. 6, pp. 1151-1221.

Corresponding author

Annegret Bendiek can be contacted at: annegret.bendiek@swp-berlin.org

Annegret Bendiek is Deputy Head at Stiftung Wissenschaft und Politik, Berlin, Germany.
Magnus Römer is Research Fellow at WZB Berlin Social Science Center, Berlin, Germany.

Received 27 July 2018
Revised 15 October 2018
Accepted 8 November 2018